South Carolina Data Breach Reveals More Than One Error In State's Data Protection Efforts

October 31, 2012 - For years, ACCESS has been advising consumers, businesses and government agencies to adopt and stick to strict data protection protocols. And over the years, it continues to amaze us that government agencies have not complied even through some of the largest data breaches ever recorded have been as a result of lacking data security within government agencies. It turns out that South Carolina's recent breach appears to fall into this category.

Tweet

(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();

(function() {
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
po.src = 'https://apis.google.com/js/plusone.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();

It is bad enough that hackers gained access to the state's Department of Revenue computer system and were able to maintain access for roughly three months before anyone noticed. As it turns out, none of the data within their computer system appears to have been encrypted. This includes the Social Security Numbers of South Carolina taxpayers.

After the breach was announced, Governor Nicki Haley was forced to admit that SSN's are not typically encrypted on state agency computer systems. The reason given for this was that encryption is "cumbersome". Of course, so is protecting your identity after it has been stolen. If you don't believe me, I'm fairly certain that there are 3.6 million residents of South Carolina who are ready to back me up on that statement.

But Haley was correct when she said, â€œThe industry standard is that most Social Security numbers are not encrypted. A lot of banks donâ€™t encrypt. A lot of those (government) agencies you might think encrypt Social Security numbers actually donâ€™t. Itâ€™s not just that this was a DOR situation, but an industry situation.â€•

In this case however, it really isn't clear that anyone would have been protected with encryption. That's because the way that the hackers logged onto the state's computer system was with legitimate compute credentials that were apparently stolen from an employee at the Department of Revenue.

That little revelation brings up an entirely new set of questions. Private companies that have highly sensitive information stored on computers will frequently force their employees to change their passwords every few weeks. It is very apparent that the state didn't do that since the hackers were able to comb through taxpayer data over a period of months.

And since the hackers were logging on using a legitimate account, even if the data on the state's systems had been encrypted, it would have been decrypted for anyone viewing it once they were logged into the system.

This isn't just an issue for residents of South Carolina. It is an issue for the entire country. This breach is revealing some significant weaknesses in the ways that states store and access data on their citizens. Agencies at all levels of government would be wise to look closely at what is happening in South Carolina, compare their systems to those of SC, and make appropriate changes to protect their citizens.

byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow me on Twitter:

Follow ACCESS